WHAT IS CLAIMED IS:

1. A mobile terminal for accessing a content server by wired and/or wireless communication, downloading content from the content server, and uploading the downloaded content to an external device, comprising:

a memory for storing model information and a serial number of the mobile terminal and the downloaded content, and also for storing an encryption key for encrypting the content downloaded from the external device;

a communication unit for providing an interface for exchanging data with the external device;

an encryption unit for encrypting the serial number and the content with the encryption key;

a controller for uploading the encrypted content to the external device via the communication unit, and for transmitting a download request signal for the uploaded content to the external device in response to an input command; and

a decryption unit for decrypting, with the encryption key, the content downloaded from the external device in response to the download request signal for the uploaded content.

2. The mobile terminal of claim 1, wherein the encryption key is generated by the external device based on the model information and the serial number of the mobile terminal.

3. The mobile terminal of claim 2, wherein the encryption key is generated by the external device considering further time information set in the external device.

4. A content security system comprising:

a mobile terminal for encrypting content provided from a content server with an encryption key provided from an external device, and for uploading the encrypted content to the external device; and

an external memory device for generating the encryption key based on model information and a serial number of the mobile terminal, and storing the encrypted content uploaded from the mobile terminal.

5. The content security system of claim 4, wherein the external memory device generates the encryption key considering further time information set in the external memory device.

6. The content security system of claim 5, wherein the external memory device determines whether the time information set in the external memory device is identical to time information set in the mobile terminal, and generates the encryption key if the time information set in the external memory device is identical to time information set in the mobile terminal.

7. The content security system of claim 4, wherein the mobile terminal transmits a download request signal for previously uploaded content to the external memory device in response to an input command, and decrypts, with the encryption key, content downloaded from the external memory device in response to the download request signal.

8. A content protection method using a content security system having a mobile terminal for downloading content from a content server and an external memory device for storing the content at a request of the mobile terminal, the method comprising the steps of:

transmitting a content upload request signal to the external memory device in response to an input command;

transmitting to the external memory device model information and a serial number of the mobile terminal, requested by the external memory device in response to the content upload request signal;

encrypting content to be uploaded with an encryption key generated by the external memory device based on the model information and the serial number; and

transmitting the content encrypted by the encryption key to the external memory device.

9. The content protection method of claim 8, further comprising the steps of:

determining whether the encrypted content uploaded from the mobile terminal is identical to the content encrypted by the encryption key; and

storing the encrypted content on the external memory device if the encrypted content

uploaded from the mobile terminal is identical to the content encrypted by the encryption key.

10. The content protection method of claim 9, further comprising the steps of:

upon receiving a download command for the previously uploaded content, transmitting a content download request signal to the external memory device;

if content index information for downloading is selected from content index information provided from the external memory device in response to the content download request signal, transmitting the selected content index information to the external memory device;

if encrypted content is downloaded from the external memory device according to the selected content index information, decrypting the downloaded encrypted content with the encryption key.

11. The content protection method of claim 8, wherein the encryption key is generated by the external memory device considering further time information set in the external memory device.

12. The content protection method of claim 11, wherein the encryption key is generated when time information set in the external memory device is identical to time information set in the mobile terminal.